- 下载volatility
- 用DumpIt工具（是内存副本获取工具）生成主机的物理内存镜像。副本文件是以*.raw为后缀的镜像文件，取证的对象就是这个内存镜像

### 使用：

(1)常用命令：imageinfo、kpcrscan、dlllist、filescan、handles、modscan、netscan、pslist、pstree。

- Imageinfo命令：用于查看我们正在分析的内存样本的摘要信息
- kpcrscan命令：用于查找内存中用于定义内核处理器控制区域（KPCR）的_KPCR结构体信息
- dlllist命令：能够显示一个进程装载的动态链接库的信息，其显示列表主要包括加载的动态链接库文件的基地址、文件大小以及文件所在路径。
- filescan命令：此命令将显示系统上的打开的文件，包括已被恶意软件隐藏的文件。
- handles命令：显示在一个进程中打开的处理。
- modscan命令：扫描_ldr_data_table_entry对象的物理内存。显示内核的驱动程序，包括已隐藏/链接的。
- netscan命令：发现TCP / UDP端点和监听器。这个命令将显示一个主动网络连接的列表。
- pslist命令：可以枚举系统中的进程，这条命令通过遍历PsActiveProcessHead指针指向的双向链表枚举当前内存中活跃的所有进程信息，主要包括偏移地址、进程ID号、父进程ID号、线程数量、句柄数量、进程会话ID号以及进程开始和退出的时间。
- pstree命令：这个命令显示跟pslist一样的信息，只是以树的形式。

## 一、volatility使用

**例题文件**

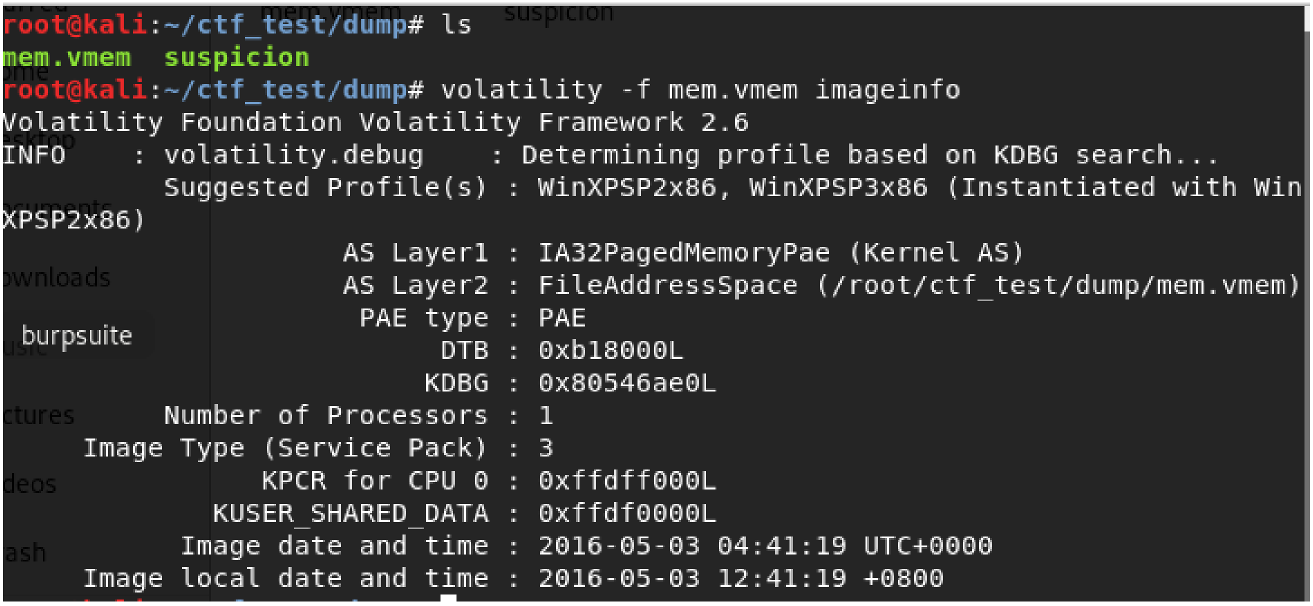
链接: http://pan.baidu.com/s/1c2BIGLE

密码: 9v2z

```
volatility -f <文件名> -profile=<配置文件> <插件> [插件参数]
```

(1)使用imageinfo插件来猜测dump文件的profile值：WinXPSP2x86

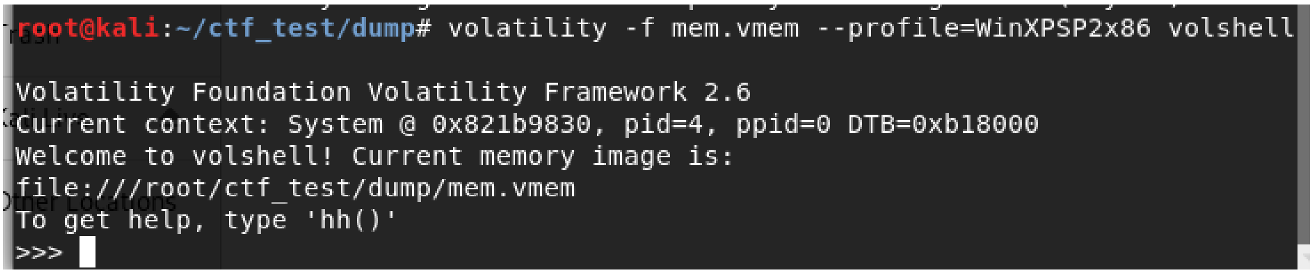
```
# volatility -f mem.vmem imageinfo
```



```
root@kali:~/ctf_test/dump# ls
mem.vmem  suspicion
root@kali:~/ctf_test/dump# volatility -f mem.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with Win
XPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/ctf_test/dump/mem.vmem)
                      PAE type : PAE
                           DTB : 0xb18000L
                          KDBG : 0x80546ae0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2016-05-03 04:41:19 UTC+0000
     Image local date and time : 2016-05-03 12:41:19 +0800
```

(2)得到profile值后可使用插件volshell执行shell命令

```
# volatility -f mem.vmem -profile=WinXPSP2x86
```



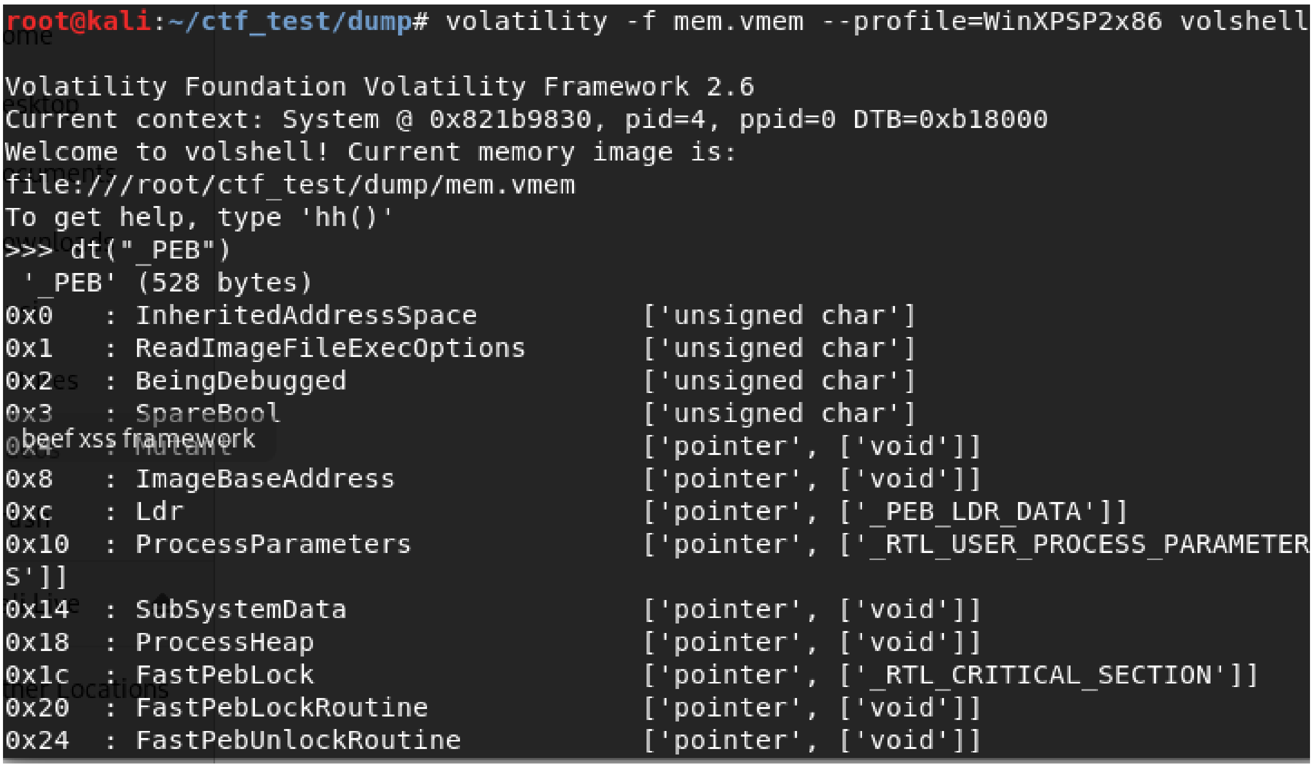
```
root@kali:~/ctf_test/dump# volatility -f mem.vmem --profile=WinXPSP2x86 volshell

Volatility Foundation Volatility Framework 2.6
Current context: System @ 0x821b9830, pid=4, ppid=0 DTB=0xb18000
Welcome to volshell! Current memory image is:
file:///root/ctf_test/dump/mem.vmem
To get help, type 'hh()'
>>> 
```

**shell的命令**

```
dt("内核关键数据结构名称")
```

如

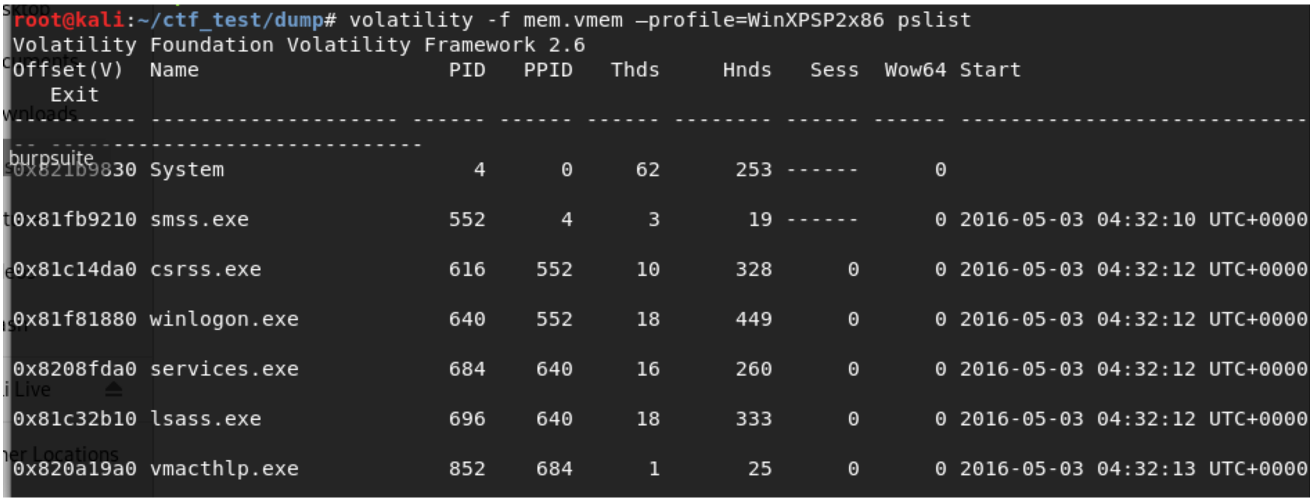
```
dt("_PEB")
```



```
root@kali:~/ctf_test/dump# volatility -f mem.vmem --profile=WinXPSP2x86 volshell

Volatility Foundation Volatility Framework 2.6
Current context: System @ 0x821b9830, pid=4, ppid=0 DTB=0xb18000
Welcome to volshell! Current memory image is:
file:///root/ctf_test/dump/mem.vmem
To get help, type 'hh()'
>>> dt("_PEB")
 '_PEB' (528 bytes)
0x0   : InheritedAddressSpace          ['unsigned char']
0x1   : ReadImageFileExecOptions       ['unsigned char']
0x2   : BeingDebugged                  ['unsigned char']
0x3   : SpareBool                      ['unsigned char']
0x4   : Mutant                         ['pointer', ['void']]
0x8   : ImageBaseAddress               ['pointer', ['void']]
0xc   : Ldr                            ['pointer', ['_PEB_LDR_DATA']]
0x10  : ProcessParameters              ['pointer', ['_RTL_USER_PROCESS_PARAMETER
S']]
0x14  : SubSystemData                  ['pointer', ['void']]
0x18  : ProcessHeap                    ['pointer', ['void']]
0x1c  : FastPebLock                    ['pointer', ['_RTL_CRITICAL_SECTION']]
0x20  : FastPebLockRoutine             ['pointer', ['void']]
0x24  : FastPebUnlockRoutine           ['pointer', ['void']]
```

**pslist列举进程**

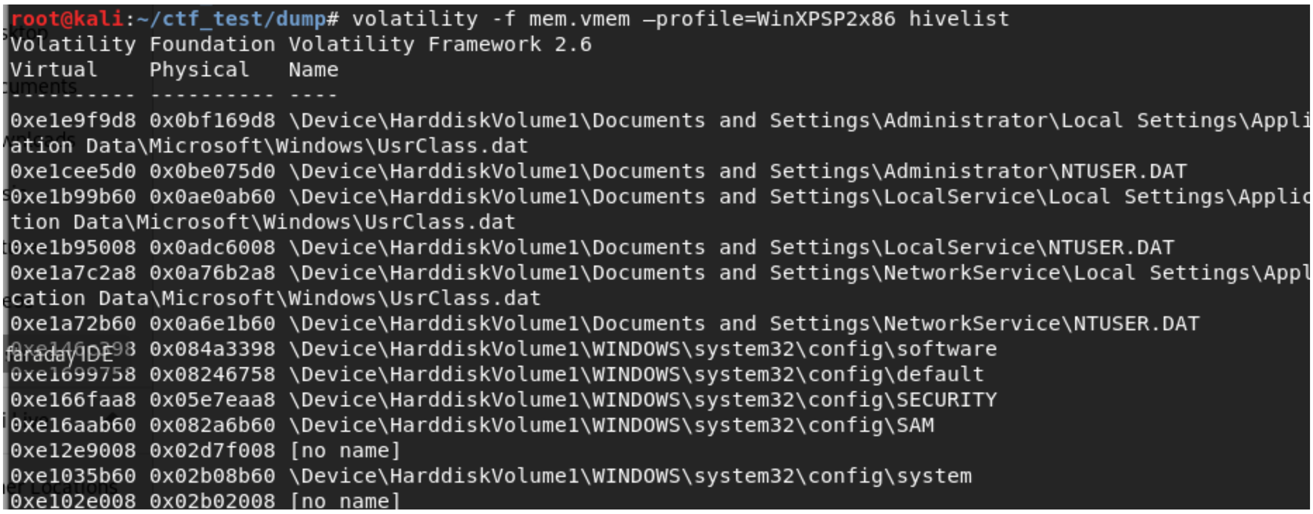
```
# volatility -f mem.vmem –profile=WinXPSP2x86 pslist
```



```
root@kali:~/ctf_test/dump# volatility -f mem.vmem –profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
   Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ----------------------------
-- ------------------------------
0x821b9830 System                    4      0     62      253 ------      0

0x81fb9210 smss.exe                552      4      3       19 ------      0 2016-05-03 04:32:10 UTC+0000

0x81c14da0 csrss.exe               616    552     10      328      0      0 2016-05-03 04:32:12 UTC+0000

0x81f81880 winlogon.exe            640    552     18      449      0      0 2016-05-03 04:32:12 UTC+0000

0x8208fda0 services.exe            684    640     16      260      0      0 2016-05-03 04:32:12 UTC+0000

0x81c32b10 lsass.exe               696    640     18      333      0      0 2016-05-03 04:32:12 UTC+0000

0x820a19a0 vmacthlp.exe            852    684      1       25      0      0 2016-05-03 04:32:13 UTC+0000
```

**列举缓存在内存的注册表**

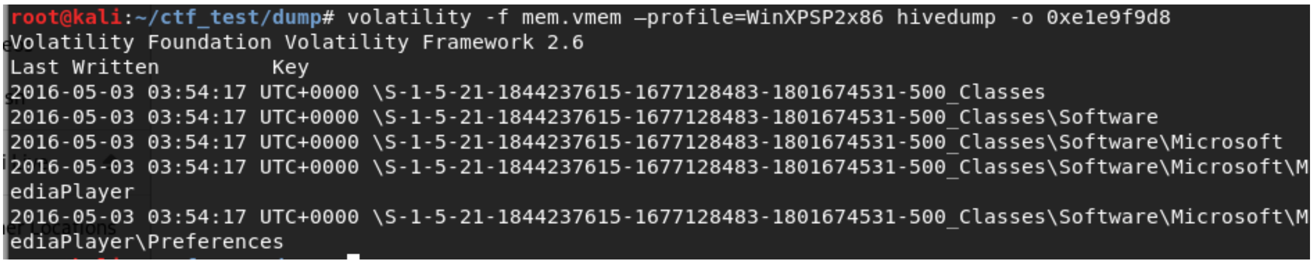
```
volatility -f mem.vmem –profile=WinXPSP2x86 hivelist
```



```
root@kali:~/ctf_test/dump# volatility -f mem.vmem —profile=WinXPSP2x86 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0xe1e9f9d8 0x0bf169d8 \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Appli
ation Data\Microsoft\Windows\UsrClass.dat
0xe1cee5d0 0x0be075d0 \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
0xe1b99b60 0x0ae0ab60 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Applic
tion Data\Microsoft\Windows\UsrClass.dat
0xe1b95008 0x0adc6008 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe1a7c2a8 0x0a76b2a8 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Appl
cation Data\Microsoft\Windows\UsrClass.dat
0xe1a72b60 0x0a6e1b60 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe146c398 0x084a3398 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe1699758 0x08246758 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe166faa8 0x05e7eaa8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0xe16aab60 0x082a6b60 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe12e9008 0x02d7f008 [no name]
0xe1035b60 0x02b08b60 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe102e008 0x02b02008 [no name]
```

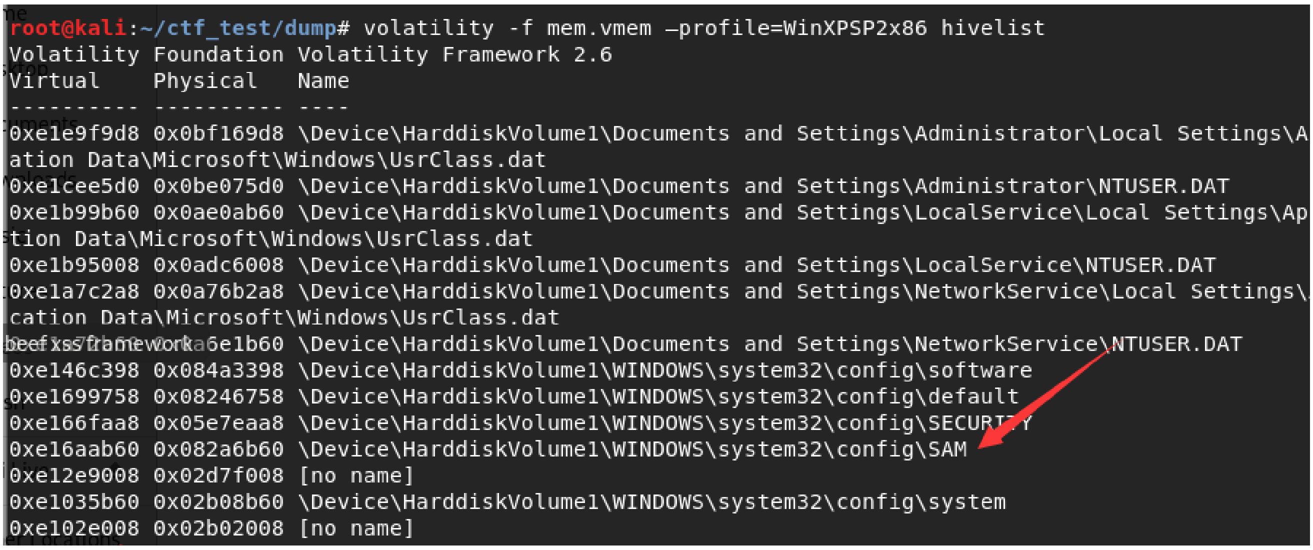
**hivedump打印出注册表中的数据：**

```
volatility -f mem.vmem –profile=WinXPSP2x86 hivedump -o <注册表的virtual地址>
```

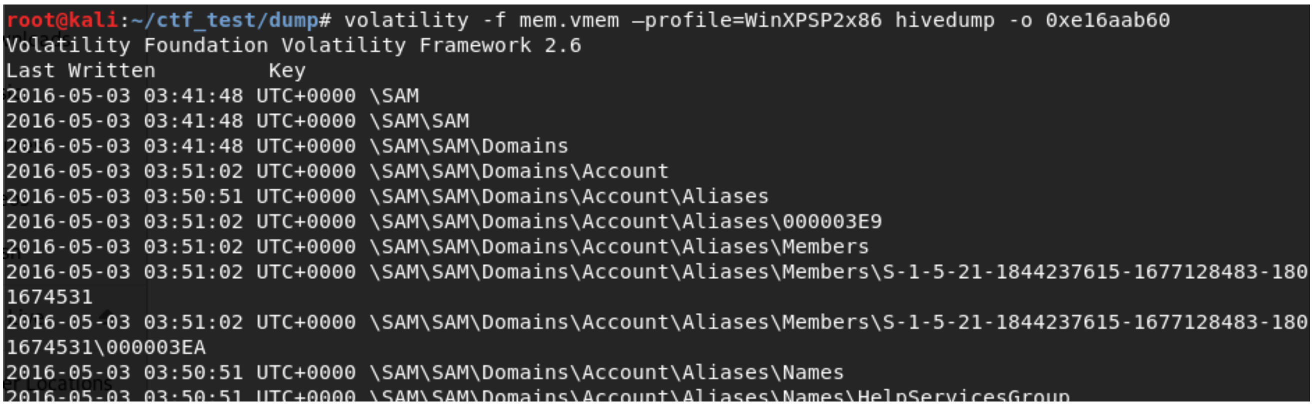


```
root@kali:~/ctf_test/dump# volatility -f mem.vmem —profile=WinXPSP2x86 hivedump -o 0xe1e9f9d8
Volatility Foundation Volatility Framework 2.6
Last Written        Key
2016-05-03 03:54:17 UTC+0000 \S-1-5-21-1844237615-1677128483-1801674531-500_Classes
2016-05-03 03:54:17 UTC+0000 \S-1-5-21-1844237615-1677128483-1801674531-500_Classes\Software
2016-05-03 03:54:17 UTC+0000 \S-1-5-21-1844237615-1677128483-1801674531-500_Classes\Software\Microsoft
2016-05-03 03:54:17 UTC+0000 \S-1-5-21-1844237615-1677128483-1801674531-500_Classes\Software\Microsoft\M
ediaPlayer
2016-05-03 03:54:17 UTC+0000 \S-1-5-21-1844237615-1677128483-1801674531-500_Classes\Software\Microsoft\M
ediaPlayer\Preferences
```

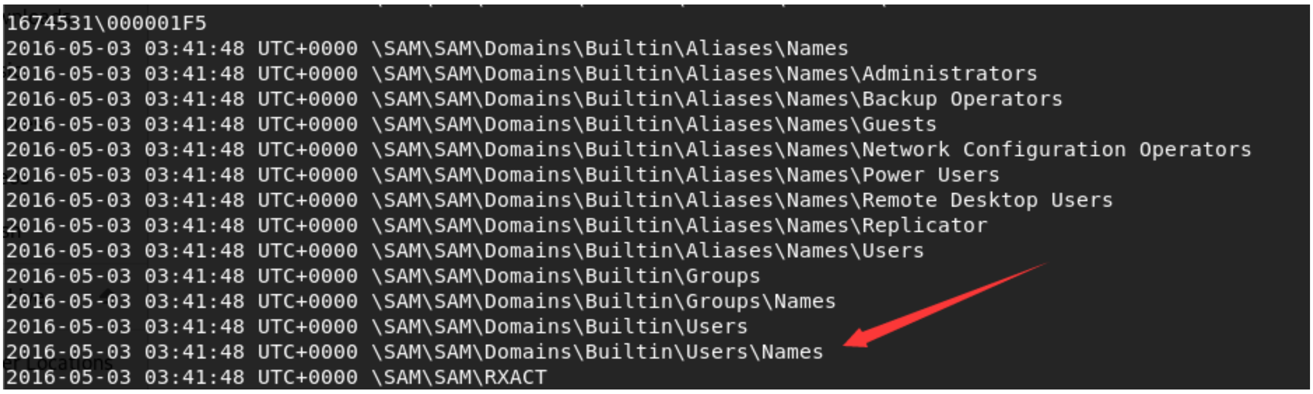
**获取SAM表中的用户：**



```
root@kali:~/ctf_test/dump# volatility -f mem.vmem —profile=WinXPSP2x86 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0xe1e9f9d8 0x0bf169d8 \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\A
ation Data\Microsoft\Windows\UsrClass.dat
0xe1cee5d0 0x0be075d0 \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
0xe1b99b60 0x0ae0ab60 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Ap
tion Data\Microsoft\Windows\UsrClass.dat
0xe1b95008 0x0adc6008 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe1a7c2a8 0x0a76b2a8 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\
cation Data\Microsoft\Windows\UsrClass.dat
0xe1a72b60 0x0a6e1b60 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe146c398 0x084a3398 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe1699758 0x08246758 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe166faa8 0x05e7eaa8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0xe16aab60 0x082a6b60 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe12e9008 0x02d7f008 [no name]
0xe1035b60 0x02b08b60 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe102e008 0x02b02008 [no name]
```



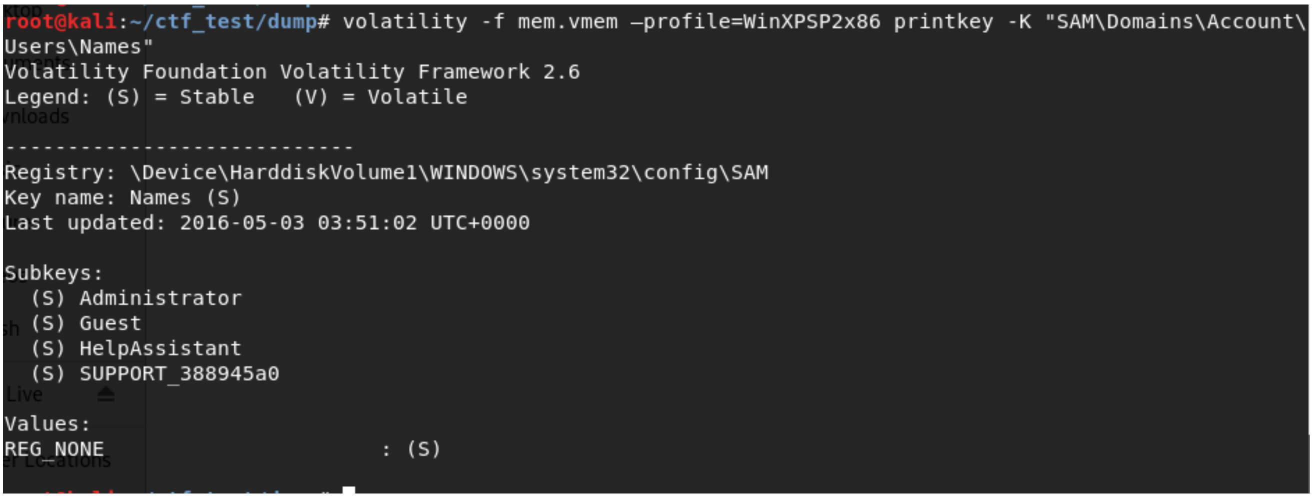
```
root@kali:~/ctf_test/dump# volatility -f mem.vmem –profile=WinXPSP2x86 hivedump -o 0xe16aab60
Volatility Foundation Volatility Framework 2.6
Last Written         Key
2016-05-03 03:41:48 UTC+0000 \SAM
2016-05-03 03:41:48 UTC+0000 \SAM\SAM
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains
2016-05-03 03:51:02 UTC+0000 \SAM\SAM\Domains\Account
2016-05-03 03:50:51 UTC+0000 \SAM\SAM\Domains\Account\Aliases
2016-05-03 03:51:02 UTC+0000 \SAM\SAM\Domains\Account\Aliases\000003E9
2016-05-03 03:51:02 UTC+0000 \SAM\SAM\Domains\Account\Aliases\Members
2016-05-03 03:51:02 UTC+0000 \SAM\SAM\Domains\Account\Aliases\Members\S-1-5-21-1844237615-1677128483-180
1674531
2016-05-03 03:51:02 UTC+0000 \SAM\SAM\Domains\Account\Aliases\Members\S-1-5-21-1844237615-1677128483-180
1674531\000003EA
2016-05-03 03:50:51 UTC+0000 \SAM\SAM\Domains\Account\Aliases\Names
2016-05-03 03:50:51 UTC+0000 \SAM\SAM\Domains\Account\Aliases\Names\HelpServicesGroup
```



```
1674531\000001F5
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Builtin\Aliases\Names
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Builtin\Aliases\Names\Administrators
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Builtin\Aliases\Names\Backup Operators
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Builtin\Aliases\Names\Guests
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Builtin\Aliases\Names\Network Configuration Operators
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Builtin\Aliases\Names\Power Users
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Builtin\Aliases\Names\Remote Desktop Users
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Builtin\Aliases\Names\Replicator
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Builtin\Aliases\Names\Users
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Builtin\Groups
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Builtin\Groups\Names
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Builtin\Users
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Builtin\Users\Names
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\RXACT
```

```
# volatility -f mem.vmem -profile=WinXPSP2x86 printkey -K
"SAM\Domains\Account\Users\Names"
```

可以看到有4个用户



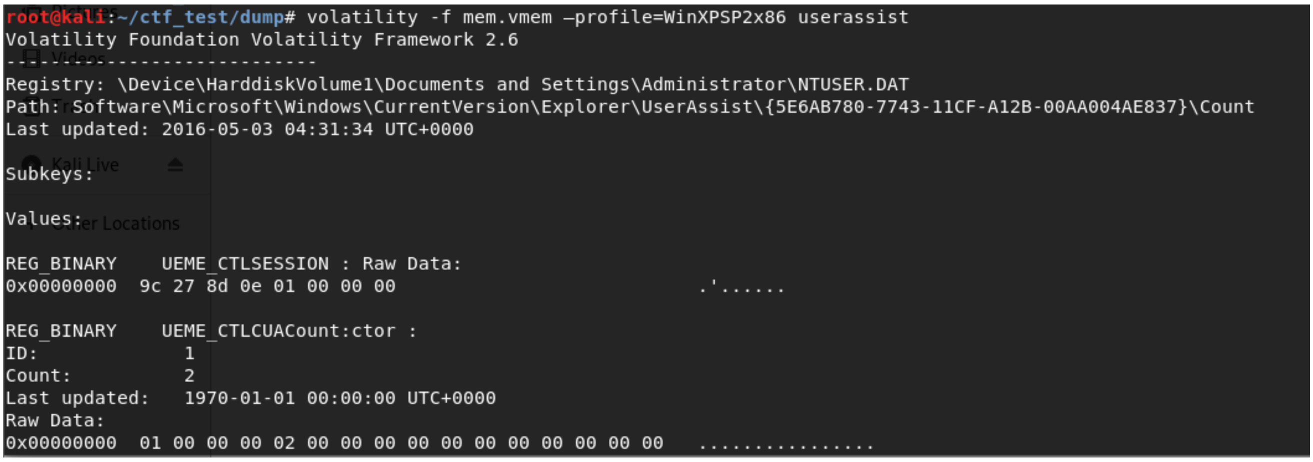
```
root@kali:~/ctf_test/dump# volatility -f mem.vmem –profile=WinXPSP2x86 printkey -K "SAM\Domains\Account\
Users\Names"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
Key name: Names (S)
Last updated: 2016-05-03 03:51:02 UTC+0000

Subkeys:
  (S) Administrator
  (S) Guest
  (S) HelpAssistant
  (S) SUPPORT_388945a0

Values:
REG_NONE                     : (S)
```

**获取最后登录系统的账户：**

```
# volatility -f mem.vmem -profile=WinXPSP2x86 printkey -K "SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon"
```

**提取出内存记录（当时正在运行的程序，运行次数，最后一次运行的时间**

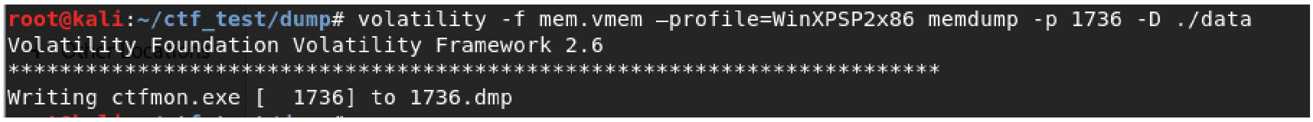
```
# volatility -f mem.vmem -profile=WinXPSP2x86 userassist
```



```
root@kali:~/ctf_test/dump# volatility -f mem.vmem –profile=WinXPSP2x86 userassist
Volatility Foundation Volatility Framework 2.6
----------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
Path: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count
Last updated: 2016-05-03 04:31:34 UTC+0000

Subkeys:

Values:

REG_BINARY    UEME_CTLSESSION : Raw Data:
0x00000000  9c 27 8d 0e 01 00 00 00                           .'......

REG_BINARY    UEME_CTLCUACount:ctor :
ID:             1
Count:          2
Last updated:   1970-01-01 00:00:00 UTC+0000
Raw Data:
0x00000000  01 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00   ................
```

**以dmp格式dump出某个进程数据**

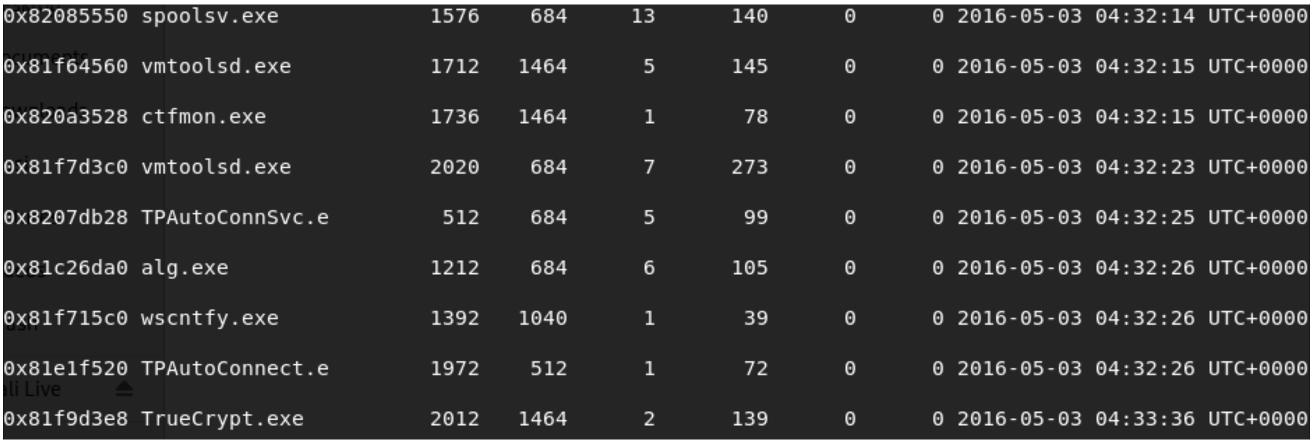
```
# volatility -f mem.vmem -profile=WinXPSP2x86 -p [PID] -D [dump出的文件保存的目录]
```



```
root@kali:~/ctf_test/dump# volatility -f mem.vmem –profile=WinXPSP2x86 memdump -p 1736 -D ./data
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing ctfmon.exe [  1736] to 1736.dmp
```

## 二、解题步骤

```
# volatility -f mem.vmem -profile=WinXPSP2x86 pslist
```

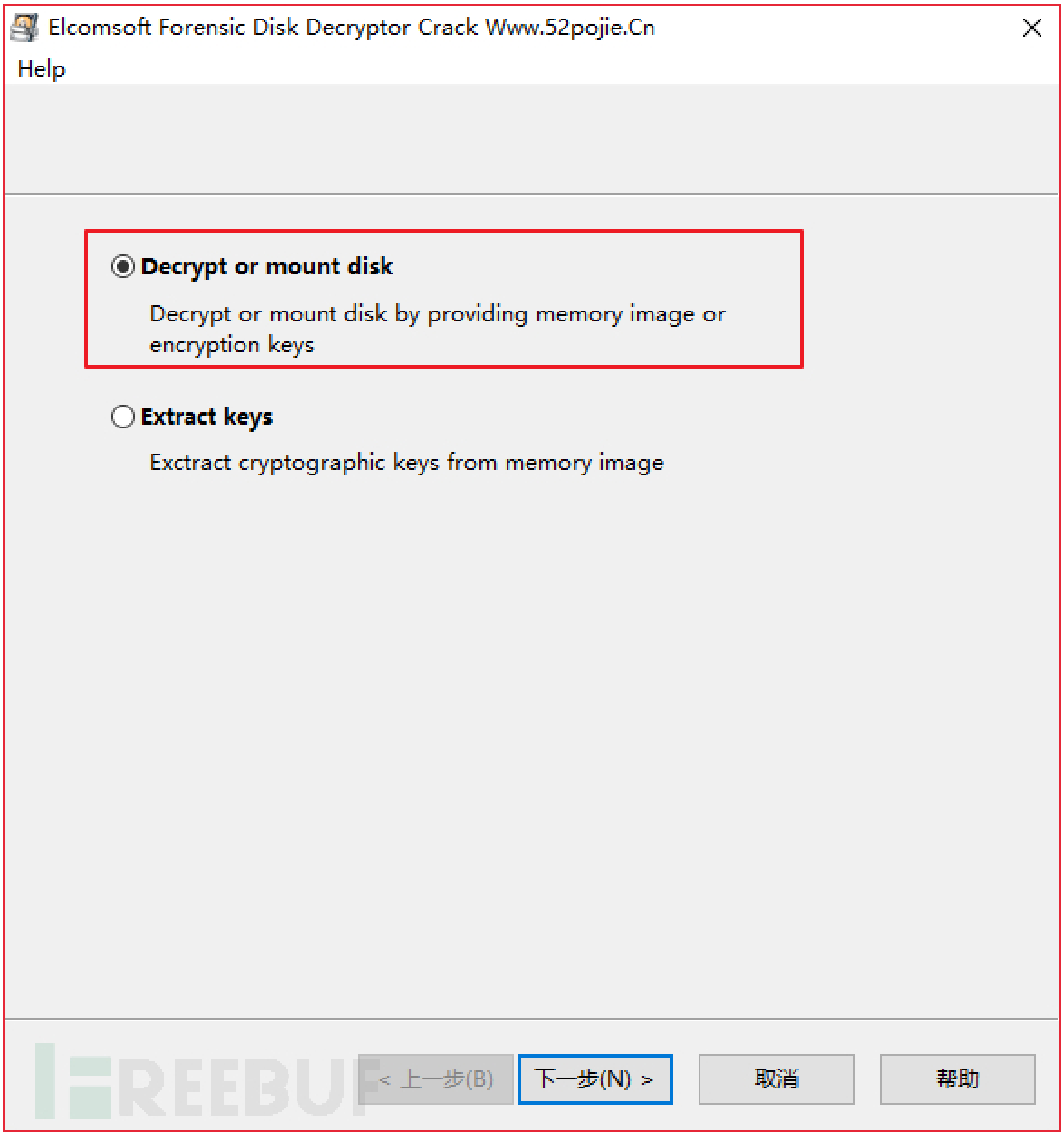


```
0x82085550 spoolsv.exe            1576    684     13      140      0      0 2016-05-03 04:32:14 UTC+0000
0x81f64560 vmtoolsd.exe           1712   1464      5      145      0      0 2016-05-03 04:32:15 UTC+0000
0x820a3528 ctfmon.exe             1736   1464      1       78      0      0 2016-05-03 04:32:15 UTC+0000
0x81f7d3c0 vmtoolsd.exe           2020    684      7      273      0      0 2016-05-03 04:32:23 UTC+0000
0x8207db28 TPAutoConnSvc.e         512    684      5       99      0      0 2016-05-03 04:32:25 UTC+0000
0x81c26da0 alg.exe                1212    684      6      105      0      0 2016-05-03 04:32:26 UTC+0000
0x81f715c0 wscntfy.exe            1392   1040      1       39      0      0 2016-05-03 04:32:26 UTC+0000
0x81e1f520 TPAutoConnect.e        1972    512      1       72      0      0 2016-05-03 04:32:26 UTC+0000
0x81f9d3e8 TrueCrypt.exe          2012   1464      2      139      0      0 2016-05-03 04:33:36 UTC+0000
```

最后一个进程TrueCrypy.exe是一款加密程序，可以推出，另一个文件suspicion为加密的结果。将进程从内存dump出来。

```
volatility -f mem.vmem -profile=WinXPSP2x86 memdump -p 1464 -D ./data
```

得到dmp文件后，需要借助Elcomsoft Forensic Disk Decryptor（Elcomsoft硬盘取证解密器，简称为EFDD）软件来获取key和破解文件



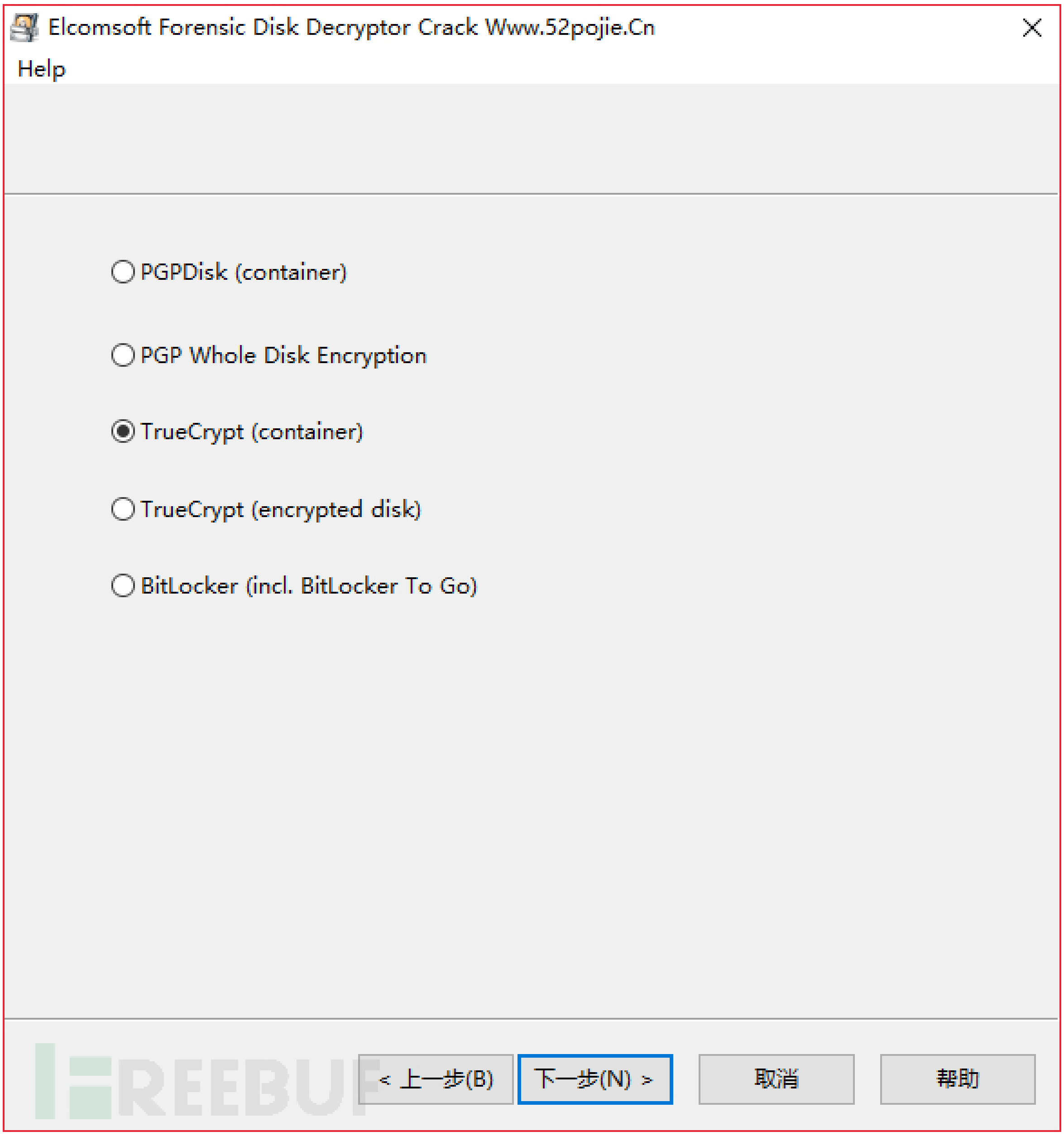
Elcomsoft Forensic Disk Decryptor Crack Www.52pojie.Cn

● **Decrypt or mount disk**

Decrypt or mount disk by providing memory image or encryption keys

○ **Extract keys**

Exctract cryptographic keys from memory image



Elcomsoft Forensic Disk Decryptor Crack Www.52pojie.Cn

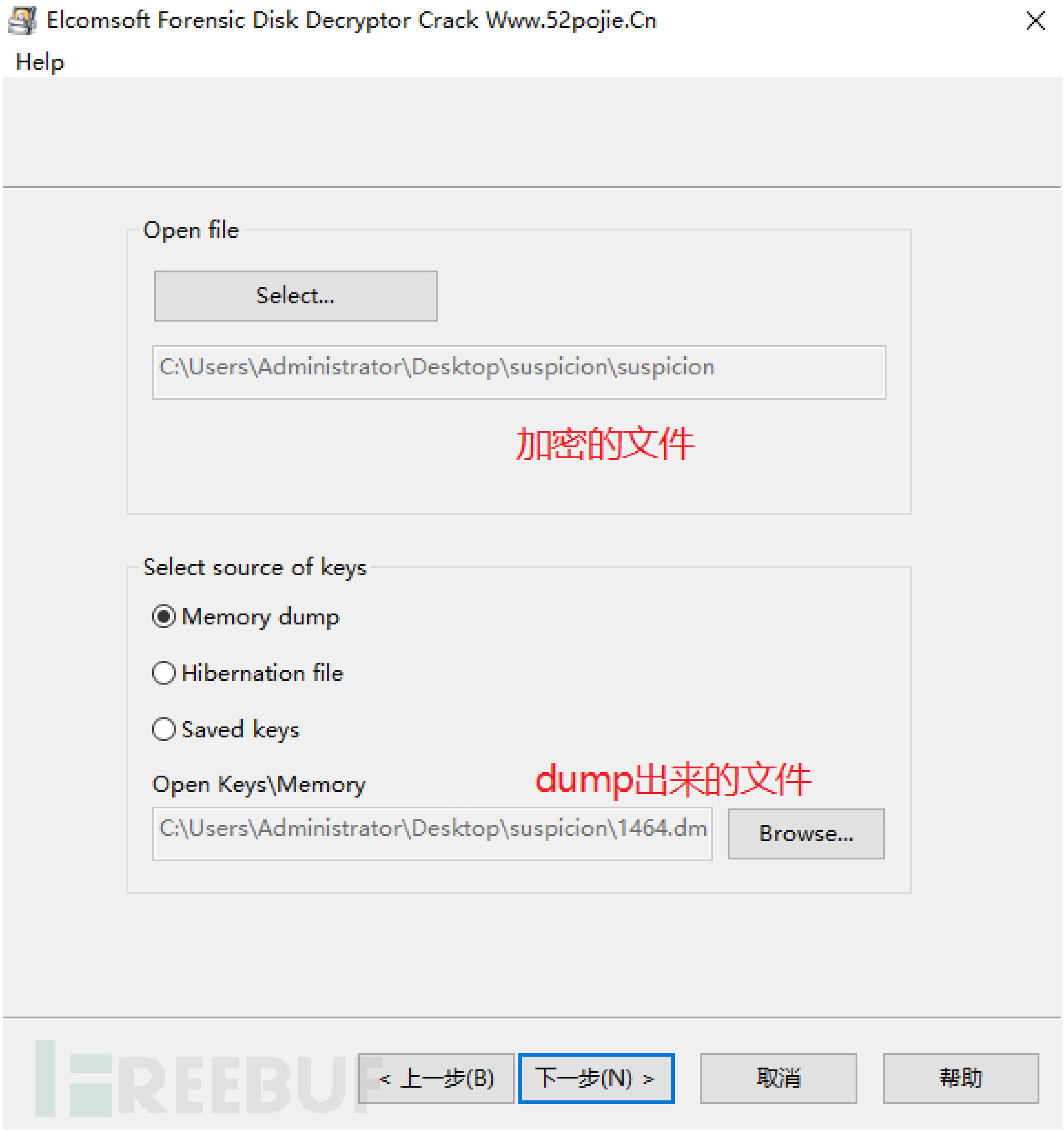
○ PGPDisk (container)

○ PGP Whole Disk Encryption

● TrueCrypt (container)

○ TrueCrypt (encrypted disk)

○ BitLocker (incl. BitLocker To Go)



Elcomsoft Forensic Disk Decryptor Crack Www.52pojie.Cn

Help

Open file

Select...

C:\Users\Administrator\Desktop\suspicion\suspicion

加密的文件

Select source of keys

● Memory dump

○ Hibernation file

○ Saved keys

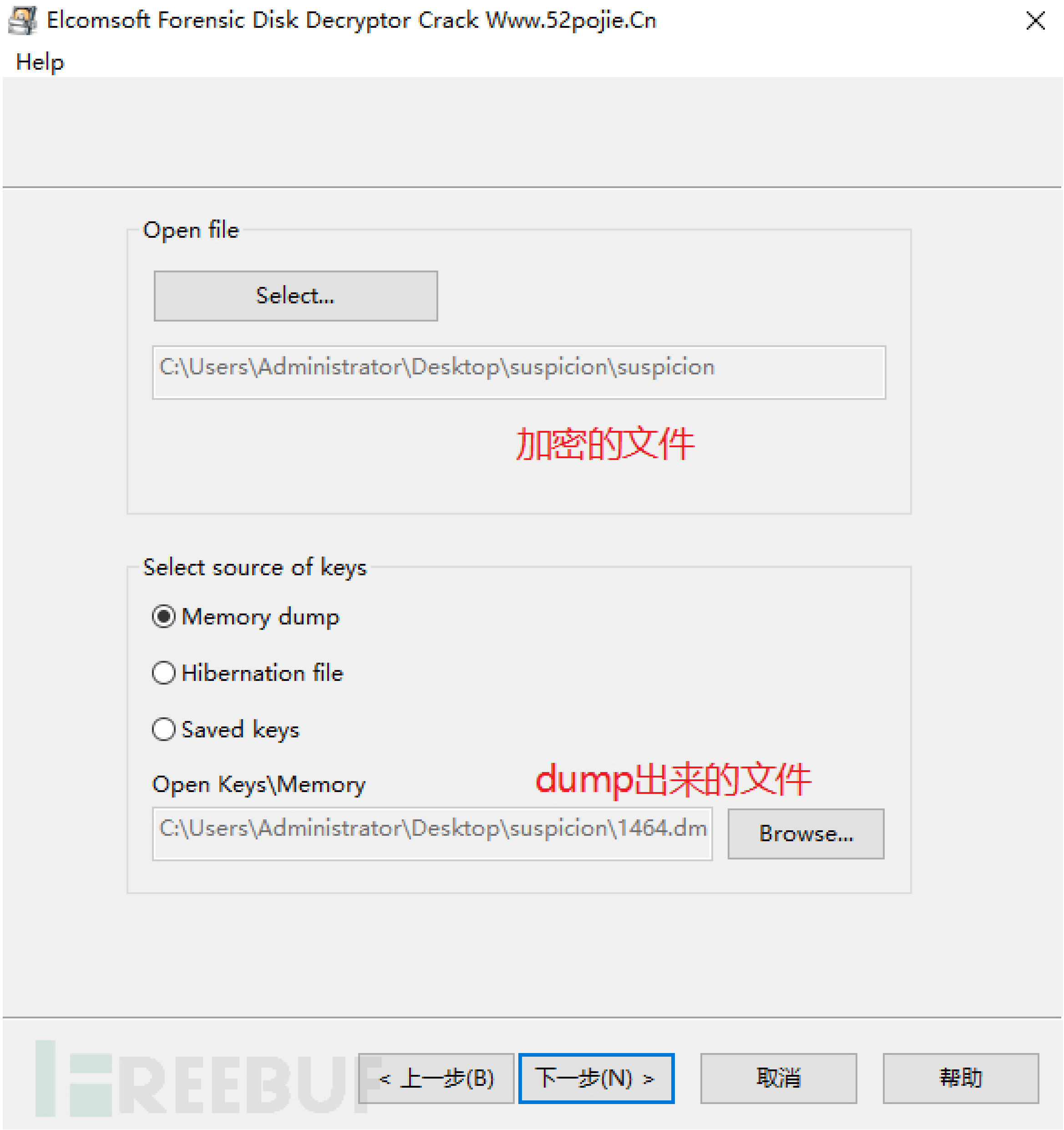
Open Keys\Memory

dump出来的文件

C:\Users\Administrator\Desktop\suspicion\1464.dm

Browse...

< 上一步(B)　下一步(N) >　取消　帮助



Open file

C:\Users\Administrator\Desktop\suspicion\suspicion

加密的文件

Select source of keys

● Memory dump

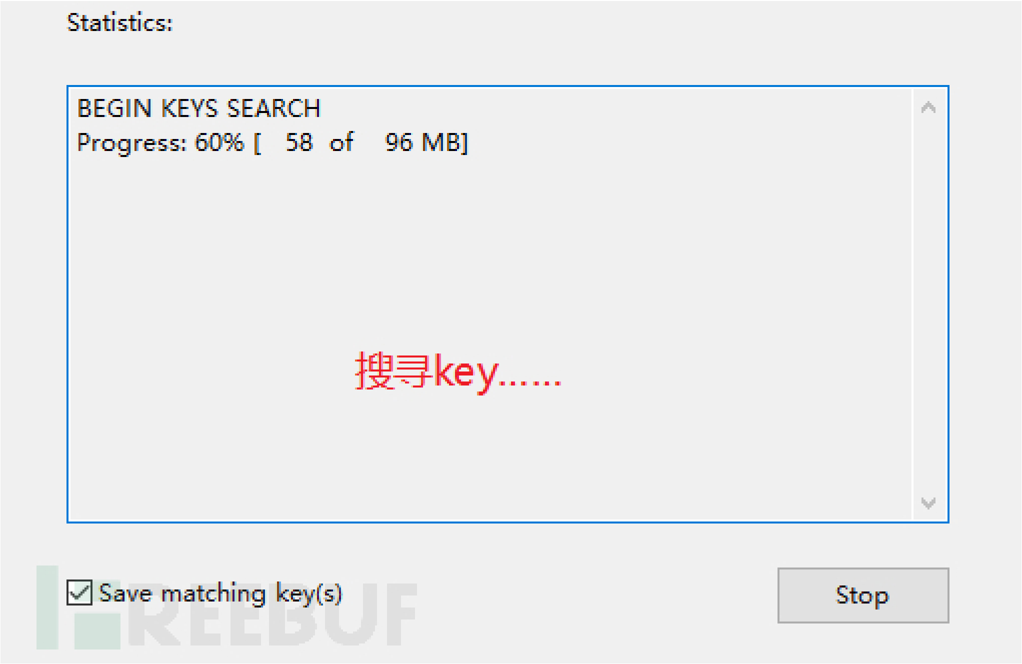
○ Hibernation file

○ Saved keys

Open Keys\Memory

C:\Users\Administrator\Desktop\suspicion\1464.dm

dump出来的文件

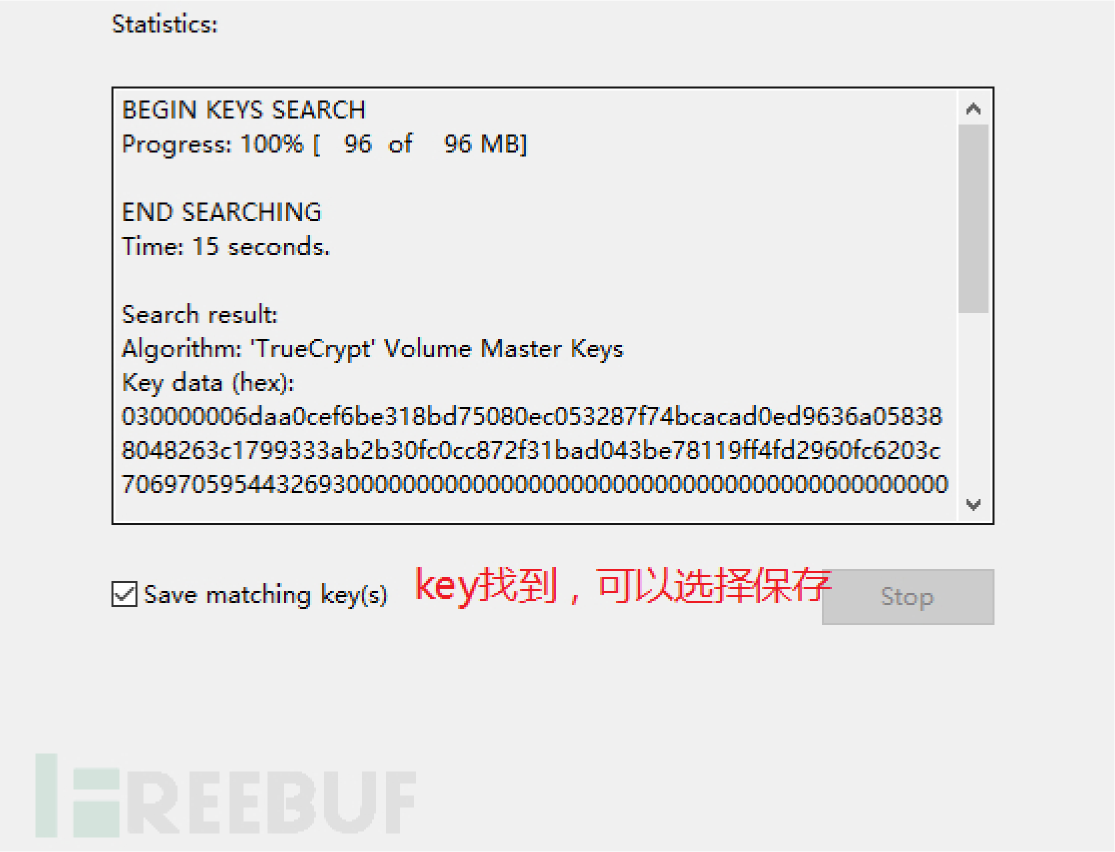


Statistics:

```
BEGIN KEYS SEARCH
Progress: 60% [   58  of    96 MB]
```

搜寻key……

☑ Save matching key(s)

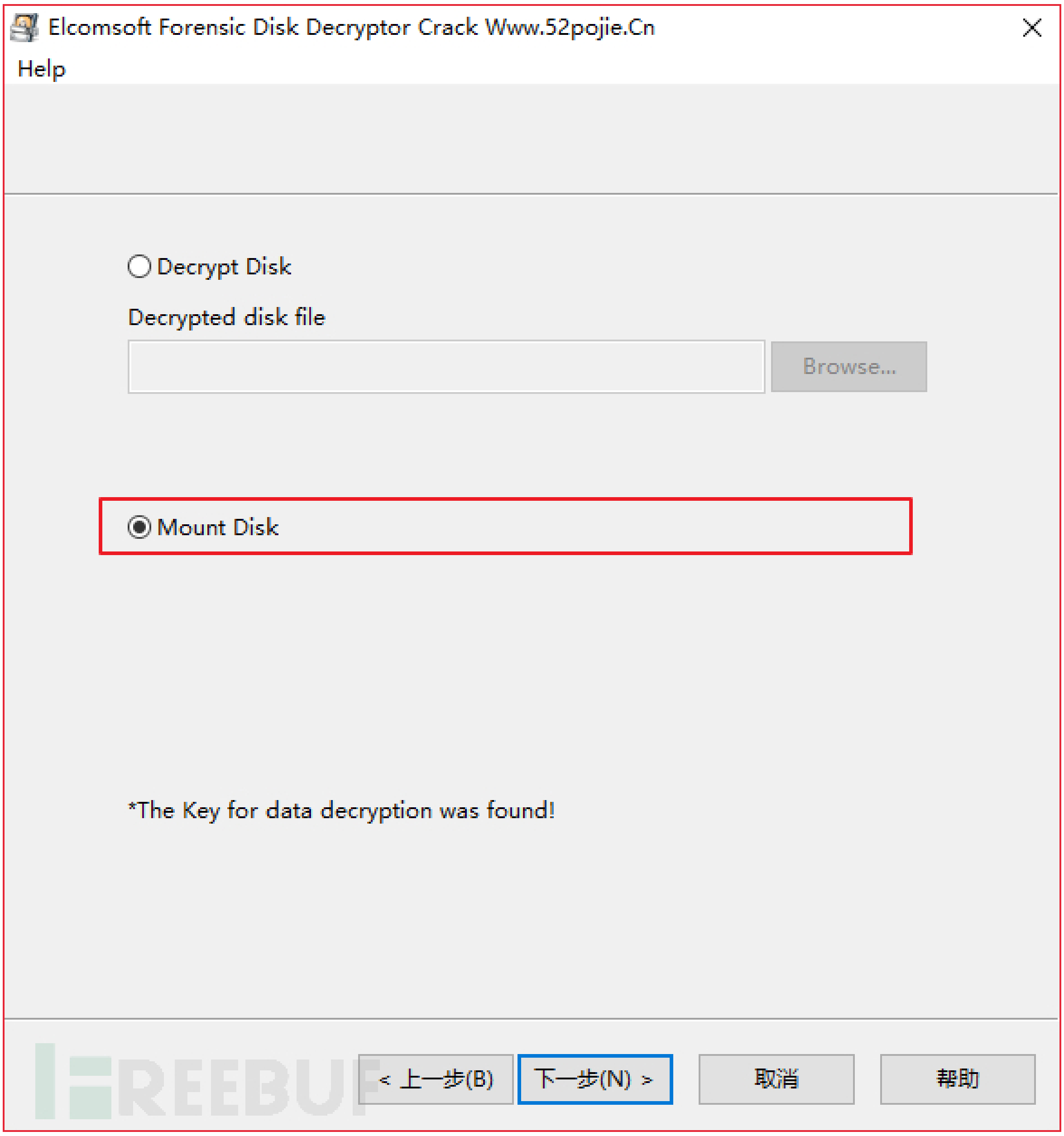


Statistics:

```
BEGIN KEYS SEARCH
Progress: 100% [   96  of    96 MB]

END SEARCHING
Time: 15 seconds.

Search result:
Algorithm: 'TrueCrypt' Volume Master Keys
Key data (hex):
030000006daa0cef6be318bd75080ec053287f74bcacad0ed9636a05838
8048263c1799333ab2b30fc0cc872f31bad043be78119ff4fd2960fc6203c
70697059544326930000000000000000000000000000000000000000
```

☑ Save matching key(s)

key找到，可以选择保存



Elcomsoft Forensic Disk Decryptor Crack Www.52pojie.Cn

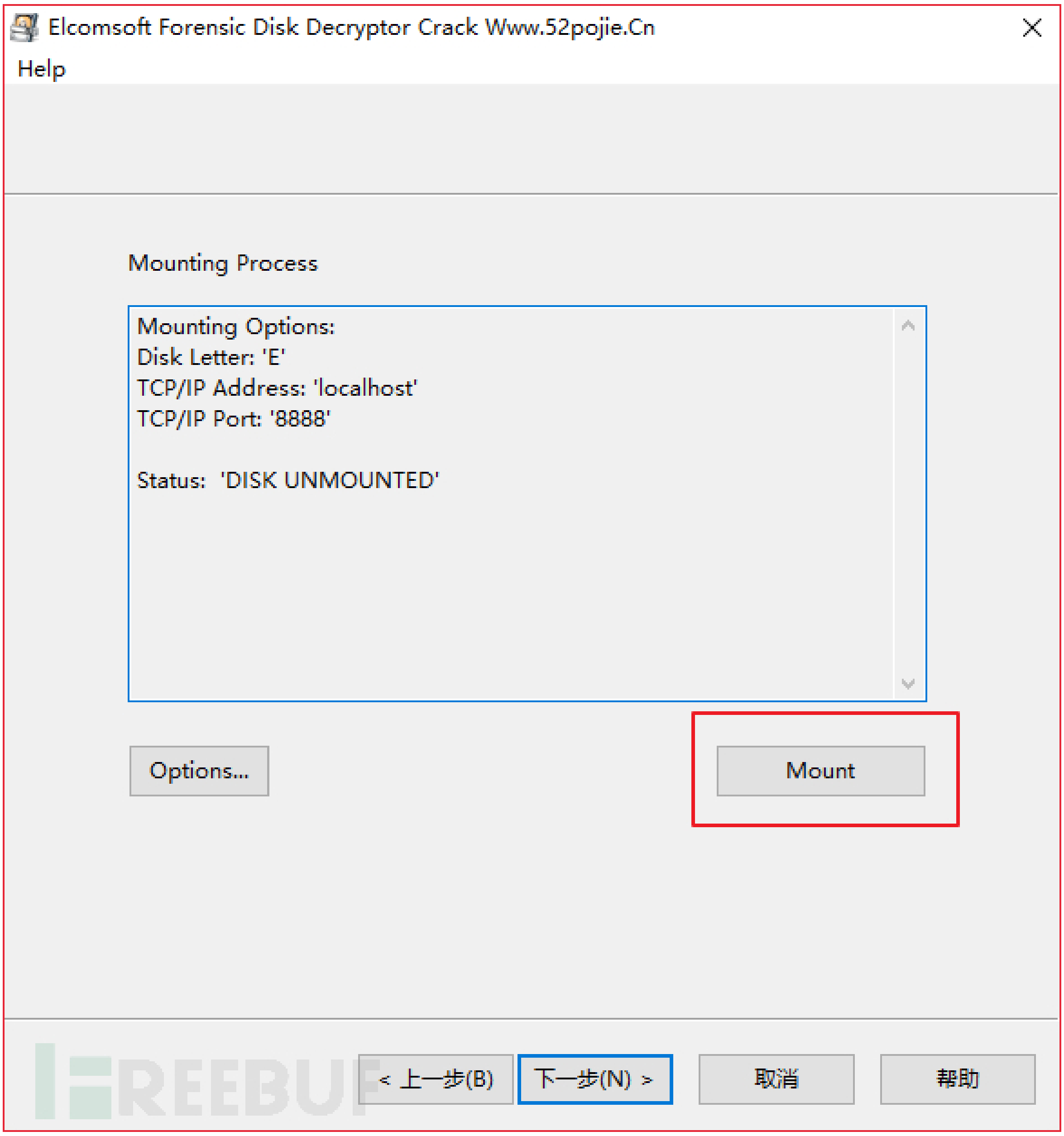
Help

○ Decrypt Disk

Decrypted disk file

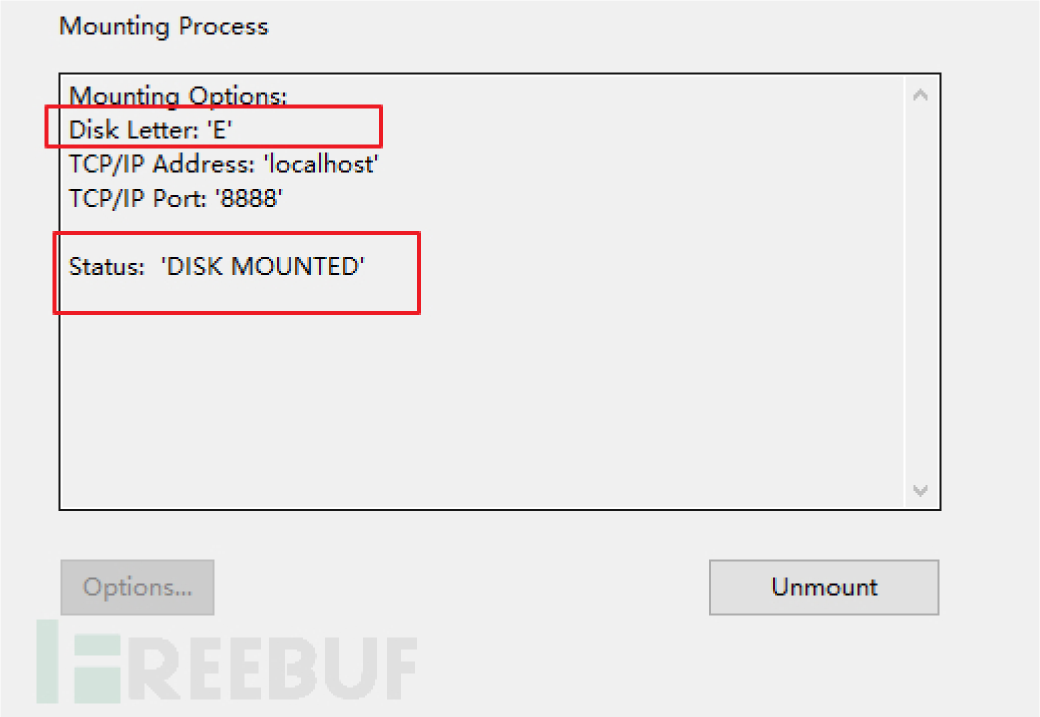
● Mount Disk

*The Key for data decryption was found!

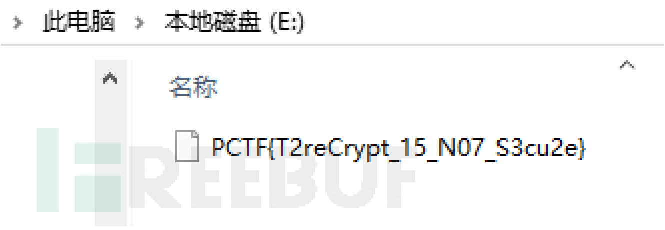


Mounting Options:
Disk Letter: 'E'
TCP/IP Address: 'localhost'
TCP/IP Port: '8888'

Status:  'DISK UNMOUNTED'



```
Mounting Options:
Disk Letter: 'E'
TCP/IP Address: 'localhost'
TCP/IP Port: '8888'

Status:  'DISK MOUNTED'
```



PCTF{T2reCrypt_15_N07_S3cu2e}